REMARKS

This response is in reply to the final Office Action ("Office Action") mailed April 14, 2010.

As a preliminary matter, Claims 15 and 16 have been amended to provide antecedent bases for some of their claim terms. No new matter has been added, and entry of these amendments is respectfully solicited.

Applicant's attorney thanks the Examiner for conducting a telephone interview on June 22, 2010. Although no agreement was reached, the present response is prepared in accordance with the discussion had during the interview to further advance the prosecution of the present application.

Claims 2, 5, 15 and 16 are currently rejected in the Office Action under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 7,441,043 to Henry et al ("Henry") in view of U.S. Patent No. 7,287,269 to Burton et al ("Burton"). Further, Claims 5, 15 and 16 are currently rejected in the Office Action under 35 U.S.C. § 103(a) as being unpatentable over Henry in view of Burton and further in view of U.S. Publication No. 2006/0185013A1 to Oyama et al ("Oyama").

Applicants respectfully assert that the present application including Claims 2, 5, 15 and 16 is in condition for allowance for the reasons discussed in detail below.

Rejections Under 35 U.S.C. § 103(a)

Claims 2, 5, 15 and 16 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Henry in view of Burton. Further, Claims 5, 15 and 16 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Henry in view of Burton and further in view of Oyama.

A *prima facie* case of obviousness may be established under section 103 if "all the claimed elements were known in the prior art and one skilled in the art could have combined the elements as claimed by known methods with no change in their respective functions, and the combination yielded nothing more than predictable results to one of ordinary skill in the art." *KSR Int'l Co. v. Teleflex, Inc.*, 550 U.S. 398 (2007); M.P.E.P. § 2143.A. Because Claims 2, 5, 15 and 16 recite combinations of features neither taught nor suggested in Henry, either alone or when combined with Burton and/or Oyama, a *prima facie* case of obviousness has not been made.

Prior to discussing why Claims 2, 5, 15 and 16 of the present application are allowable over prior arts, a brief description of exemplary embodiments of the present invention is set forth below. It should be understood that the following is provided merely to assist the Examiner's understanding of the present invention and is not intended to limit the scope of the claims.

With the conventional network system, to establish a tunnel by key exchange of IPsec main mode, a mobile wireless terminal apparatus needs to know in advance the IP address of a virtual private network relay apparatus, and the virtual private network relay apparatus needs to know in advance the IP address of the mobile wireless terminal apparatus at its moving destination. However, when IPsec is applied to a mobile environment where a mobile wireless terminal apparatus freely moves between a public network and private network, the IP address of the mobile wireless terminal apparatus changes every time it moves, making it difficult to exchange an IPsec key by IPsec main mode. One solution is to establish the IPsec tunnel by an IPsec key exchange in aggressive mode, wherein an IPsec user ID is communicated between networks without being encrypted. With the aggressive mode, however, degradation in security becomes a problem. (See the publication of the present application, U.S. Patent Application Publication No. 2008/0232382, page 1, paragraphs [0009] and [0010].)

To solve this problem among other problems, the present invention according to various exemplary embodiments utilizes a connection authentication server installed on the public wireless LAN system, which authenticates connection of a mobile wireless terminal apparatus to the public wireless LAN system. According to various exemplary embodiments of the present invention, the mobile wireless terminal apparatus is configured to acquire an IP address of a virtual private network relay apparatus from the connection authentication server when the connection to the public wireless LAN system is permitted. (See FIG. 1.) The mobile wireless terminal apparatus sends its IP address (i.e., the IP address of the mobile wireless terminal apparatus) to the virtual private network relay apparatus, via the connection authentication server, so that the mobile wireless terminal apparatus and the virtual private network relay apparatus can start key exchange by IPsec main mode using the IP address of each other. According to this configuration, since the IP addresses of the mobile wireless terminal apparatus and the virtual private network relay apparatus are transmitted using the secure communication path established

between the mobile wireless terminal apparatus and the connection authentication server, it is possible to prevent deterioration in security. (See the publication, page 5, paragraphs [0058] and [0059].)

Now turning to the claims of the present application, Claims 2, 5, 15 and 16 explicitly recite the features of the present invention discussed above. Specifically, Claims 2 and 5 recite a mobile wireless terminal apparatus, in a mobile wireless communication system comprising "a connection authentication server that is installed on the public wireless LAN system and authenticates connection of the mobile wireless terminal apparatus to the public wireless LAN system," wherein the mobile wireless terminal apparatus comprises "an address acquiring section that acquires an IP address of the virtual private network relay apparatus from the connection authentication server when the connection to the public wireless LAN system is permitted,' "an address notifying section that sends an IP address of the mobile wireless terminal apparatus to the virtual private network relay apparatus, via the connection authentication server," and "an IPsec key exchanging section that performs an IPsec key exchange [or exchange of the IPsec key] with the virtual private network relay apparatus using the IP address of the virtual private network relay apparatus [or the IPsec pre-shared secret key, both acquired from the connection authentication server]." Similarly, Claims 15 and 16 recite a mobile wireless terminal apparatus comprising "an authentication processing section that performs authentication processing for connection to a public wireless LAN system and to a connection authentication server," "an address acquiring section that acquires an IP address of a virtual private network relay apparatus from the connection authentication server when the connection to the public wireless LAN system is permitted," "an address notifying section that sends an IP address of the mobile wireless terminal apparatus to the virtual private network relay apparatus, via the connection authentication server," and "an IPsec key exchanging section that performs an IPsec key exchange [or exchange of the IPsec key] with the virtual private network relay apparatus using the IP address of the virtual private network relay apparatus [or the IPsec pre-shared secret key, both acquired from the connection authentication server]."

Claims 2, 5, 15 and 16 are Allowable.

In the Office Action, it is asserted that Henry teaches each and every element recited in Claims 2, 5, 15 and 16, except that Henry fails to teach that "the IPsec key exchange is performed by IPsec main mode" as recited in Claim 2. (See Office Action, pages 4 and 5.) It is then asserted that Burton, col. 8 lines 13-44 and col.9 lines 2-11, teaches this element missing in Henry. (See Office Action, pages 4 and 5.)

Specifically, it is asserted that Henry teaches the mobile wireless terminal apparatus comprising "an address acquiring section that acquires an IP address of the virtual private network relay apparatus from the connection authentication server when the connection to the public wireless LAN system is permitted" (col. 10, lines 60-67 and col. 17, lines 1-13), "an address notifying section that sends an IP address of the mobile wireless terminal apparatus to the virtual private network relay apparatus, via the connection authentication server" (col. 10, lines 60-67 and col. 17, lines 1-10), and "an IPsec key exchanging section that performs an IPsec key exchange with the virtual private network relay apparatus" (col. 9, lines 54-56, col. 11, lines 14-38, col. 12, lines 3-5, and col. 18, lines 40-49). (See Office Action, page 4, first three paragraphs.) Applicants respectfully disagree.

In Henry, a mobile wireless terminal apparatus acquires its local IP address from the WLAN using DHCP (col. 9, lines 54-56). On the other hand, it appears that Henry's mobile wireless terminal apparatus is already aware of (or preset with) an IP address of a secure mobility gateway ("IP_{SMG}"). See Henry, col. 16, line 62-col. 17, line 14--"the IRC [in the user's computer] obtains a local IP address for the user's computer … denoted as IP_{local}.... The user's computer sends an IP packet to an IP host…. At 600 the IRC encapsulates this IP packet in a UDP packet, in which the source and destination IP addresses are IP_{local} and IP_{SMG} respectively." Therefore, there simply is no need or desirability for the mobile wireless terminal apparatus of Henry to acquire the IP_{SMG} from another entity, such as from a RADIUS server or AAA that the Examiner has asserted as corresponding to the claimed "connection authentication server." Henry does not teach or suggest that its mobile network access device 200 ("a mobile wireless terminal apparatus") acquires an IP address of the SMG 238 ("IP_{SMG}") from the RADIUS server or AAA when the connection of the mobile network access device 200 to the public wireless

LAN system is permitted. In other words, Henry does not at all teach or suggest from where the mobile network access device 200 acquires the IP_{SMG} at what timing, presumably because in Henry the IP_{SMG} is preset in the mobile network access device 200.

Therefore, Henry does not teach or suggest a mobile wireless terminal apparatus comprising "an address acquiring section that acquires an IP address of a virtual private network relay apparatus from the connection authentication server when the connection to the public wireless LAN system is permitted" and "an address notifying section that sends an IP address of the mobile wireless terminal apparatus to the virtual private network relay apparatus, via the connection authentication server" (emphasis added), as claimed in the present application.

Henry describes that "the IRC [in the user's computer] creates an IPsec tunnel with the IPsec gateway using the IKE (Internet Key Exchange) protocol." (See Henry, col. 9, lines 54-56.) However, Henry fails to disclose that the mobile network access device 200 performs an IPsec key exchange with the IPsec gateway using the IP address of the SMG 238 [or the"IPsec pre-shared secret key"] that was acquired from the RADIUS server or AAA when the connection of the mobile network access device 200 to the public wireless LAN system is permitted. Therefore, Henry also fails to teach a mobile wireless terminal apparatus comprising "an IPsec key exchanging section that performs an IPsec key exchange [or exchange of the IPsec key] with the virtual private network relay apparatus using the IP address of the virtual private network relay apparatus [or the IPsec pre-shared secret key, both acquired from the connection authentication server]," as further claimed in the present application.

Regarding Burton, applicants merely note that Burton fails to remedy the deficiency of Henry with respect to each of the claim elements discussed above and missing in Henry.

For at least the reasons discussed above, neither Henry nor Burton, either alone or in combination, teaches or renders obvious each and every element of Claims 2, 5, 15 and 16. As a result, a *prima facie* case of obviousness has not been established relative to Claims 2, 5, 15 and 16. Applicants respectfully request withdrawal of the 35 U.S.C. § 103(a) rejection of Claims 2, 5, 15 and 16 based on Henry and Burton.

Oyama describes utilizing an Authorizing, Authentication, Accounting (AAA) server to transfer HMIPv6-related information required for authenticating and authorizing a mobile node

for HMIPv6 service over the AAA infrastructure. (See abstract.) Regarding Oyama, applicants again merely note that it too fails to teach or suggest the subject matter missing in Henry, that is, "an address acquiring section that acquires an IP address of a virtual private network relay apparatus from the connection authentication server when the connection to the public wireless LAN system is permitted," "an address notifying section that sends an IP address of the mobile wireless terminal apparatus to the virtual private network relay apparatus, via the connection authentication server," and "an IPsec key exchanging section that performs an IPsec key exchange [or exchange of the IPsec key] with the virtual private network relay apparatus using the IP address of the virtual private network relay apparatus [or the IPsec pre-shared secret key, both acquired from the connection authentication server]," as recited in Claims 5, 15 and 16. As such, Oyama cannot cure the deficiency of Henry and Burton. Therefore, Henry, Burton and Oyama, either alone or in any combination, fail to teach or suggest all of the elements recited in Claims 5, 15 and 16, and accordingly fail to establish a *prima facie* case of obviousness against Claims 5, 15 and 16. Applicants respectfully request withdrawal of this basis of rejection of Claims 5, 15 and 16 under 35 U.S.C. § 103(a).

CONCLUSION

In light of the foregoing remarks, applicants assert that the claims of the present application recite combinations of features neither disclosed nor rendered obvious by the prior art. Therefore, applicants respectfully request early and favorable action allowing all pending claims. If any further questions remain, the Examiner is invited to telephone applicants' attorney at the number listed below.

Respectfully submitted,

SEED Intellectual Property Law Group PLLC

/Shoko Leek/
Shoko I. Leek
Registration No. 43,746

SIL:jrh

701 Fifth Avenue, Suite 5400
Seattle, Washington 98104
Phone: (206) 622-4900
Fax: (206) 682-6031

1634407_1.DOC